9-17-8

PATENT
ATTORNEYDOCKET: 206,443

47982 appeal brief v1 7/09/08

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Anat BREMLER BAR, et al.	Examiner: Thuong Nguyen
Serial No.:	10/774,169	Group Art Unit: 2155
Filed:	February 5, 2004	
For:	DETECTING AND PROTECTING AGAINST WORM TRAFFIC ON A NETWORK	

September 15, 2008

STATEMENT OF FILING BY EXPRESS MAIL 37 C.F.R. § 1.10

This correspondence is being deposited with the U.S. Postal Service on **September 15, 2008** in an envelope as "Express Mail Post Office to Addressee" Mailing Label No. **EB 908 953 515 US** Addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPEAL BRIEF

This Appeal Brief is submitted further to the Notice of Appeal filed on July 15, 2008.

A check in the amount of $510.00 is enclosed to cover the cost of filing the Appeal Brief under 37 C.F.R.§ 41.20(b)(2).

Please charge any othr fees which may be due to our Deposit Account No. 01-0035.

09/17/2008 CNGUYEN2 00000088 10774169
01 FC:1402 510.00 OP

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is Cisco Technology, Inc., assignee of all rights to the present Application.

RELATED APPEALS AND INTERFERENCES

There are no other related appeals and interferences known to Applicants or to the real party in interest.

STATUS OF CLAIMS

Claims 1, 4-24, 29-35, 38-58, 63-69, 72-92 and 97-108 are pending. The application was filed with 102 claims. Claims 103-108 have been added in the response filed on July 19, 2006. Claims 2-3, 27, 36-37, 61, 70-71 and 95 have been cancelled in the response filed July 19, 2006. Claims 25-26, 28, 59-60, 62, 93-94 and 96 have been cancelled in the response after final filed October 10, 2007.

Claims 1, 4-24, 29-35, 38-58, 63-69, 72-92 and 97-108 are being appealed.

STATUS OF AMENDMENTS

An amendment after final was filed on October 10, 2007, in which claims 25-26, 28, 59-60, 62, 93-94 and 96 were cancelled.

SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1, 35 and 69

The present invention includes, as recited in claims 1, 35 and 69, respectively, a method, apparatus and a computer software product for processing communication traffic that is directed to a group of addresses on a network, including identifying a subset of the group of the addresses such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group, monitoring the communication traffic that is directed to the addresses in the subset, determining respective baseline characteristics of the communication traffic that is directed to each of the addresses in the subset, detecting a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the subset, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin and responsively to detecting the deviation, filtering the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin. The method, apparatus and computer software product for processing communication traffic of the present invention is shown in Figs. 1 and 2 and described in the description thereof.

The method for processing communication traffic that is directed to a group of addresses on a network of the present invention, as recited in claim 1, includes:

identifying a subset of the group of the addresses [Fig. 2, step 50] such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group [page 19, lines 10-12];

monitoring the communication traffic that is directed to the addresses in the subset [Fig. 2, step 62, page 22, lines 15-24];

determining respective baseline characteristics of the communication traffic that is directed to each of the addresses in the subset [page 22, lines 25-29];

detecting a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the subset, wherein the

deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin [Fig. 2, steps 64, 66; page 23, line 18-page 24, line 2]; and

responsively to detecting the deviation, filtering the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin [Fig. 2, step 70, page 16, lines 24-29, page 25, lines 24-29].

The apparatus for processing communication traffic that is directed to a group of addresses on a network of the present invention, as recited in claim 35, includes:

a guard device [guard device 28, Fig. 1], which is adapted to identify a selected subset of the group of the addresses [Fig. 2, step 50] such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group [page 19, lines 10-12], to monitor the communication traffic that is directed to the addresses in the subset [Fig. 2, step 62; page 22, lines 15-24], to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the subset [page 22, lines 25-29], to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the subset, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin [Fig. 2, steps 64, 66; page 23, line 18-page 24,line 2], and responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin [Fig. 2, step 70, page 16, lines 24-29, page 25, lines 24-29].

The computer software product for processing communication traffic that is directed to a group of addresses on a network of the present invention, as recited in claim 69, includes:

a computer-readable medium in which program instructions are stored [page 17, lines 8-16], which instructions, when read by a computer, cause the computer to identify a selected subset of the group of the addresses [Fig. 2, step 50] such that the

addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group [page 19, lines 10-12], to monitor the communication traffic that is directed to the addresses in the subset [Fig. 2, step 62; page 22, lines 15-24], to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the subset [page 22, lines 25-29], to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the subset, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin [Fig. 2, steps 64, 66; page 23, line 18-page 24, line 2], and responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin [Fig. 2, step 70, page 16, lines 24-29, page 25, lines 24-29].

Claims 29, 63 and 97

The present invention also includes, as recited in claims 29, 63 and 97, respectively, a method, apparatus and a computer software product for processing communication traffic, including monitoring the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection, detecting an increase in a rate of arrival of the packets that are indicative of the communication failure and responsively to the increase, filtering the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection. The method, apparatus and computer software product for processing communication traffic of the present invention is shown in Figs. 1 and 2 and described in the description thereof.

The method for processing communication traffic that is directed to a group of addresses on a network of the present invention, as recited in claim 29, includes:

monitoring the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection [Fig. 2, step 62; page 24, lines 8-10];

detecting an increase in a rate of arrival of the packets that are indicative of the communication failure [Fig. 2, steps 64, 66; page 21, lines 9-12]; and

responsively to the increase, filtering the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection [Fig. 2, step 70; page 16, lines 24-29, page 25, lines 24-29].

The apparatus for processing communication traffic of the present invention, as recited in claim 63, includes:

a guard device [guard device 28, Fig. 1], which is adapted to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection [Fig. 2, step 62, page 24, lines 8-10], to detect an increase in a rate of arrival of the packets that are indicative of the communication failure [Fig. 2, steps 64,66; page 21, lines 9-12], and responsively to the increase, to filter the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection [Fig. 2, step 70, page 16, lines 24-29, page 25, lines 24-29].

The computer software product of the present invention, as recited in claim 97, includes:

a computer-readable medium in which program instructions are stored [page 17, lines 8-16], which instructions, when read by a computer, cause the computer to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection [Fig. 2, step 62; page 24, lines 8-10], to detect an increase in a rate of arrival of the packets that are indicative of the communication failure [Fig. 2, steps 64, 66; page 21, lines 9-12], and responsively to the increase, to filter the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection [Fig. 2, step 70, page 16, lines 24-29, page 25, lines 24-29].

Claims 32, 66 and 100

The present invention also includes, as recited in claims 32, 66 and 100, respectively, a method, apparatus and computer software product for processing communication traffic, including monitoring the communication traffic on a network so as to detect ill-formed packets, making a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection and responsively to the determination, filtering the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection. The method, apparatus and computer software product for processing communication traffic of the present invention is shown in Figs. 1 and 2 and described in the description thereof.

Thus, the method for processing communication traffic that is directed to a group of addresses on a network of the present invention, as recited in claim 32, includes:

monitoring the communication traffic on a network so as to detect ill-formed packets [Fig. 2, step 62; page 21, lines 17-25];

making a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection [Fig. 2, steps 64, 66; page 21, lines 23-25]; and

responsively to the determination, filtering the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection [Fig. 2, step 70; page 16, lines 24-29, page 25, lines 24-29].

The apparatus for processing communication traffic of the present invention, as recited in claim 66, includes:

a guard device [guard device 28, Fig. 1], which is adapted to monitor the communication traffic on a network so as to detect ill-formed packets [Fig. 2, step 62; page 21, lines 17-25], to make a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm

infection [Fig. 2, steps 64, 66; page 21, lines 23-25], and responsively to the determination, to filter the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection[Fig. 2, step 70, page 16, lines 24-29, page 25, lines 24-29].

The computer software product of the present invention, as recited in claim 100, includes:

a computer-readable medium in which program instructions are stored [page 17, lines 8-16], which instructions, when read by a computer, cause the computer to monitor the communication traffic on a network so as to detect ill-formed packets[Fig. 2, step 62; page 21, lines 17-25], to make a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection [Fig. 2, steps 64, 66; page 21, lines 23-25], and responsively to the determination, to filter the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection [Fig. 2, step 70, page 16, lines 24-29, page 25, lines 24-29].

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed are as follows:

1) Rejection of independent claims 1, 35 and 69 under 35 U.S.C. 103(a) over Lyle in view of Smithson

2) Rejection of independent claims 29, 63 and 97 under 35 U.S.C. 103(a) over Lyle in view of Smithson

3) Rejection of independent claims 32, 66 and 100 under 35 U.S.C. 103(a) over Lyle in view of Smithson.

Applicants believe that the Examiner's application of the prior art is not appropriate and that the present claims are novel and non-obvious over the art cited by the Examiner.

ARGUMENTS

1) Rejection of independent claims 1, 35 and 69 under 35 U.S.C. 103(a) over Lyle in view of Smithson

Claims 1, 35 and 69, respectively, recite a method, apparatus and software product for processing communication traffic that is directed to a group of addresses on a network, based on monitoring traffic that is directed to a subset of the group. The subset of the group of the addresses that is to be monitored is identified such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group. The Examiner acknowledged in the Official Action (page 3, lines 11-13) that Lyle does not teach this claim limitation. In fact, Lyle neither teaches nor suggests any criterion for selection of ports or addresses to be monitored.

The Examiner went on to maintain that Smithson (Fig. 2; col. 4, lines 5-25; col. 5, lines 7-23) teaches identifying a subset of a group of addresses that are expected to receive smaller amounts of communication traffic. Fig. 2, however, shows no more than a conventional computer architecture. The passages cited by the Examiner in cols. 4 and 5 relate to measurement parameters for detecting a virus outbreak and associated user-controlled threshold levels. The parameters may include numbers of various types of e-mail messages that are sent by the monitored computer or e-mail throughput (col. 4, lines 26-39). If one of these parameters is greater than the threshold, a virus outbreak signal is generated (col. 5, lines 15-17).

Smithson is concerned with the numbers of e-mail messages that are transmitted by a single computer. He does not attempt to determine which addresses on a network receive greater or smaller amounts of communication traffic than others, nor does he suggest that such a determination might be of value in virus detection. He does not relate to choosing addresses to be monitored for purposes of virus detection or any other purpose. Thus, he certainly does not even hint at identifying or choosing to monitor certain addresses that are expected to receive **smaller** amounts of communication traffic, as recited in claims 1, 35 and 69.

The Examiner has failed to point out even a hint of teaching or motivation in either Lyle or Smithson that would have led a person of ordinary skill in the art to choose any particular subset of addresses for monitoring, let alone the surprising choice of identifying low-traffic addresses for this purpose, as recited in claims 1, 35 and 69.

Therefore, independent claims 1, 35 and 69 are patentable over the cited art.

2) Rejection of independent claims 29, 63 and 97 under 35 U.S.C. 103(a) over Lyle in view of Smithson

Claims 29, 63 and 97, respectively, recite a method, apparatus and software product in which communication traffic is monitored so as to detect packets indicative of a network communication failure that is characteristic of a worm infection. Upon detecting an increase in the rate of arrival of these packets, the communication traffic is filtered so as to remove communication traffic that is generated by the worm infection. Applicants pointed out in response to a previous Official Action and in the previous PABRR in this case that Lyle neither teaches nor suggests applying this sort of packet detection criterion. (See Appellant's Response to Official Action filed December 7, 2006, pages 6-7.)

Nevertheless, in the present Official Action (page 8, lines 11-12), the Examiner simply repeated her earlier assertion that Lyle teaches "detecting an increase in a rate of arrival of the packets that are indicative of the communication failure" in col. 10, line 60 – col. 11, line 1. This passage, however, relates only to detecting the "level or rate" of "certain types of messages" (col. 10, lines 55-59), without specifying the types of messages that are involved. Lyle makes no mention or suggestion of communication failures or how they should be handled, and does not even hint that packets indicative of such failures could be used in filtering worm-generated traffic as required by the present claims.

Smithson also says nothing about packets that are indicative of a communication failure in the network. The passage cited by the Examiner in Smithson in relation to claim 29 (col. 6, lines 34-43) proposes only that some or all e-mail attachments be blocked in case of a virus outbreak. Smithson neither teaches nor suggests detecting packets of any particular type, let alone detecting packets that are indicative of a communication failure that is characteristic of a worm infection, as recited in claims 29, 63 and 97.

Therefore, independent claims 29, 63 and 97 are patentable over the cited art.

3). Rejection of independent claims 32, 66 and 100 under 35 U.S.C. 103(a) over Lyle in view of Smithson

Claims 32, 66 and 100, respectively, recite a method, apparatus and software product in which communication traffic on a network is monitored so as to detect ill-formed packets. The ill-formed packets are used in determining that at least a portion of the traffic has been generated by a worm infection. Appellant pointed out in the above-mentioned response of December 7, 2006, and in the previous PABRR that Lyle fails to relate in any way to whether packets are well formed or ill formed, and certainly does not suggest that detection of ill-formed packets might be used in determining that a worm infection has occurred.

Yet again the Examiner has simply repeated the previous grounds of rejection. In the present Official Action, the Examiner stated (page 9, lines 12-14) that in col. 7, lines 9-19, "Lyle discloses that the method of scanning the network for the suspicious data within the tracking system." The cited passage, however, says only that "the sniffers search for data indicating an actual or suspected attack... as described more fully below." Lyle goes on to describe a number of ways in which the sniffers may search for such attack-related data (see, for example, col. 10, lines 30-59). None of these ways has anything to do with ill-formation of packets.

Smithson, likewise, says nothing at all about whether packets are well formed or ill formed, and thus could not possibly be taken to suggest detecting or making any other use of ill-formed packets.

Therefore, independent claims 32, 66 and 100 are patentable over the cited art.

Summary and Conclusion

As discussed hereinabove, Applicants respectfully submit that the prior art of Lyle and Smithson, alone and in combination, does not show or suggest, the methods, apparatuses and computer software products of the present invention as recited in independent claims 1, 29, 32, 35, 63, 66, 69, 97 and 100.

Inasmuch as the independent claims of the present invention are deemed patentable over the cited prior art, Applicants respectfully submit that the dependent claims, which depend directly or ultimately from one of the above independent claims are also patentable over the cited prior art. Therefore, as discussed hereinabove, all of the claims of the present invention are novel and non-obvious over the art cited by the Examiner.

Respectfully submitted,

ABELMAN, FRAYNE & SCHWAB
Attorneys for Applicant

By _____
Jay S. Cinamon
Attorney for Applicant
Reg. No. 24,156

666 Third Avenue
New York, NY 10017-5621
Tel.: (212) 949-9022
Fax: (212) 949-9190

CLAIMS APPENDIX

This Appendix includes all claims in their present state.

1. A method for processing communication traffic that is directed to a group of addresses on a network, comprising:

identifying a subset of the group of the addresses such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group;

monitoring the communication traffic that is directed to the addresses in the subset;

determining respective baseline characteristics of the communication traffic that is directed to each of the addresses in the subset;

detecting a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the subset, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin; and

responsively to detecting the deviation, filtering the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin.

2.-3. (Cancelled)

4. The method according to claim 1, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic.

5. The method according to claim 1, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed.

6. The method according to claim 1, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic.

7. The method according to claim 1, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group.

8. The method according to claim 1, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic.

9. The method according to claim 8, wherein detecting the deviation comprises reading a Time-To-Live (TTL) field in Internet Protocol headers of data packets sent to the addresses in the group, and detecting a change in values of the TTL field relative to the baseline characteristics.

10. The method according to claim 1, wherein detecting the deviation comprises detecting events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network.

11. The method according to claim 10, wherein detecting the events comprises detecting failures to establish a Transmission Control Protocol (TCP) connection.

12. The method according to claim 1, and comprising receiving packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to receiving the packets.

13. The method according to claim 12, wherein receiving the packets comprises receiving Internet Control Message Protocol (ICMP) unreachable packets.

14. The method according to claim 1, wherein monitoring the communication traffic comprises making a determination that one or more packets

transmitted over the network are ill-formed, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to the ill-formed packets.

15. The method according to claim 1, wherein detecting the deviation comprises incrementing a count of events that are indicative of the malicious origin of the communication traffic, and deciding whether to filter the communication traffic responsively to the count.

16. The method according to claim 15, wherein detecting the deviation comprises receiving data packets of potentially malicious origin, each data packet having a respective source address and destination address, and wherein incrementing the count comprises determining an amount by which to increment the count responsively to a given data packet depending upon whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address as the given data packet.

17. The method according to claim 16, wherein determining the amount by which to increment the count comprises incrementing the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address as the given data packet.

18. The method according to claim 1, wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein filtering the communication traffic comprises intercepting the communication traffic of the detected type.

19. The method according to claim 18, wherein detecting the type comprises determining at least one of a communication protocol and a port that is characteristic of the communication traffic.

20. The method according to claim 18, wherein detecting the type comprises determining one or more source addresses of the communication traffic that

appears to be of the malicious origin, and intercepting the communication traffic sent from the one or more source addresses.

21. The method according to claim 1, wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein monitoring the communication traffic comprises collecting specific information relating to the traffic of the detected type.

22. The method according to claim 21, wherein collecting the specific information comprises determining one or more source addresses of the traffic of the detected type.

23. The method according to claim 1, wherein monitoring and filtering the communication traffic comprise monitoring and filtering the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

24. The method according to claim 23, and comprising monitoring the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program.

25.-28. (Cancelled)

29. A method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection;

detecting an increase in a rate of arrival of the packets that are indicative of the communication failure; and

responsively to the increase, filtering the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection.

30. The method according to claim 29, wherein monitoring the communication traffic comprises detecting Internet Control Message Protocol (ICMP) unreachable packets.

31. The method according to claim 29, wherein monitoring the communication traffic comprises detecting failures to establish a Transmission Control Protocol (TCP) connection.

32. A method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect ill-formed packets;

making a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection; and

responsively to the determination, filtering the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection.

33. The method according to claim 32, wherein the packets comprise a header specifying a communication protocol, and wherein monitoring the communication traffic comprises determining that the packets contain data that are incompatible with the specified communication protocol.

34. The method according to claim 32, wherein the packets comprise a header specifying a packet length, and wherein monitoring the communication traffic comprises determining that the packets contain an amount of data that is incompatible with the specified packet length.

35. Apparatus for processing communication traffic that is directed to a group of addresses on a network, comprising a guard device, which is adapted to identify a selected subset of the group of the addresses such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group, to monitor the communication traffic that is directed to the

addresses in the subset, to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the subset, to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the subset, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin, and responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin.

36.-37. (Cancelled)

38. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic.

39. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed.

40. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic.

41. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group.

42. The apparatus according to claim 35, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic.

43. The apparatus according to claim 42, wherein the guard device is adapted to read a Time-To-Live (TTL) field in Internet Protocol headers of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems.

44. The apparatus according to claim 35, wherein the guard device is adapted to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network.

45. The apparatus according to claim 44, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection.

46. The apparatus according to claim 35, wherein the guard device is adapted to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets.

47. The apparatus according to claim 46, wherein the packets comprises Internet Control Message Protocol (ICMP) unreachable packets.

48. The apparatus according to claim 35, wherein the guard device is adapted to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets.

49. The apparatus according to claim 35, wherein the guard device is adapted to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count.

50. The apparatus according to claim 49, wherein the guard device is coupled to receive data packets of potentially malicious origin, each data packet having a respective source address and destination address, and is adapted to determine an amount by which to increment the count responsively to a given data packet depending upon whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address as the given data packet.

51. The apparatus according to claim 40, wherein the guard device is adapted to increment the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address as the given data packet.

52. The apparatus according to claim 35, wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type.

53. The apparatus according to claim 52, wherein the type of the communication traffic that appears to be of the malicious origin is characterized by at least one of a communication protocol and a port.

54. The apparatus according to claim 52, wherein the guard device is adapted to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses.

55. The apparatus according to claim 35, wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to monitor the communication traffic so as to collect specific information relating to the traffic of the detected type.

56. The apparatus according to claim 55, wherein the specific information comprises one or more source addresses of the traffic of the detected type.

57. The apparatus according to claim 35, wherein the guard device is adapted to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

58. The apparatus according to claim 57, wherein the guard device is adapted to monitor the communication traffic that is transmitted by computers in the

protected area so as to detect an infection of one or more of the computers by a malicious program.

59.-62. (Cancelled)

63. Apparatus for processing communication traffic, comprising a guard device, which is adapted to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection, to detect an increase in a rate of arrival of the packets that are indicative of the communication failure, and responsively to the increase, to filter the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection.

64. The apparatus according to claim 63, wherein the guard device is adapted to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure.

65. The apparatus according to claim 63, wherein the guard device is adapted to detect failures to establish a Transmission Control Protocol (TCP) connection.

66. Apparatus for processing communication traffic, comprising a guard device, which is adapted to monitor the communication traffic on a network so as to detect ill-formed packets, to make a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection, and responsively to the determination, to filter the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection.

67. The apparatus according to claim 66, wherein the packets comprise a header specifying a communication protocol, and wherein the guard device is adapted to detect that the packets contain data that are incompatible with the specified communication protocol.

68. The apparatus according to claim 66, wherein the packets comprise a header specifying a packet length, and wherein the guard device is adapted to detect that the packets contain an amount of data that is incompatible with the specified packet length.

69. A computer software product for processing communication traffic that is directed to a group of addresses on a network, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to identify a selected subset of the group of the addresses such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group, to monitor the communication traffic that is directed to the addresses in the subset, to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the subset, to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the subset, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin, and responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin.

70.-71. (Canceled)

72. The product according to claim 69, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic.

73. The product according to claim 69, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed.

74. The product according to claim 69, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic.

75. The product according to claim 69, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group.

76. The product according to claim 69, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic.

77. The product according to claim 76, wherein instructions cause the computer to read a Time-To-Live (TTL) field in Internet Protocol headers of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems.

78. The product according to claim 69, wherein the instructions cause the computer to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network.

79. The product according to claim 78, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection.

80. The product according to claim 69, wherein the instructions cause the computer to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets.

81. The product according to claim 80, wherein the packets comprises Internet Control Message Protocol (ICMP) unreachable packets.

82. The product according to claim 69, wherein the instructions cause the computer to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets.

83. The product according to claim 69, wherein the instructions cause the computer to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count.

84. The product according to claim 83, wherein when the computer is coupled to receive data packets of potentially malicious origin, each data packet having a respective source address and destination address, the instructions cause the computer to determine an amount by which to increment the count responsively to a given data packet depending upon whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address as the given data packet.

85. The product according to claim 84, wherein the instructions cause the computer to increment the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address as the given data packet.

86. The product according to claim 69, wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type.

87. The product according to claim 86, wherein the type of the communication traffic that appears to be of the malicious origin is characterized by at least one of a communication protocol and a port.

88. The product according to claim 86, wherein the instructions cause the computer to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses.

89. The product according to claim 69, wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to monitor the communication traffic so as to collect specific information relating to the traffic of the detected type.

90. The product according to claim 89, wherein the specific information comprises one or more source addresses of the traffic of the detected type.

91. The product according to claim 69, wherein the instructions cause the computer to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

92. The product according to claim 91, wherein the instructions cause the computer to monitor the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program.

93.-96. (Cancelled)

97. A computer software product, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection, to detect an increase in a rate of arrival of the packets that are indicative of the communication failure, and responsively to the increase, to filter the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection.

98. The product according to claim 97, wherein the instructions cause the computer to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure.

99. The product according to claim 97, wherein the instructions cause the computer to detect failures to establish a Transmission Control Protocol (TCP) connection.

100. A computer software product, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the communication traffic on a network so as to detect ill-formed packets, to make a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection, and responsively to the determination, to filter the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection.

101. The product according to claim 100, wherein the packets comprise a header specifying a communication protocol, and wherein the instructions cause the computer to detect that the packets contain data that are incompatible with the specified communication protocol.

102. The product according to claim 100, wherein the packets comprise a header specifying a packet length, and wherein the instructions cause the computer to detect that the packets contain an amount of data that is incompatible with the specified packet length.

103. The method according to claim 1, wherein identifying the subset comprises selecting clients for inclusion in the subset while excluding servers.

104. The method according to claim 1, wherein identifying the subset comprises selecting trap addresses that are not used by actual computers for inclusion in the subset.

105. The apparatus according to claim 35, wherein the subset includes clients while excluding servers.

106. The apparatus according to claim 35, wherein the subset includes trap addresses that are not used by actual computers.

107. The product according to claim 69, wherein the subset includes clients while excluding servers.

108. The product according to claim 69, wherein the subset includes trap addresses that are not used by actual computers.

EVIDENCE APPENDIX

No evidence pursuant to 37 CFR 1.130, 1.131, 1.132 or entered by or relied upon by the Examiner is being submitted.

RELATED PROCEEDINGS APPENDIX

No related proceedings are referenced in section II above, hence copies of decisions in related proceedings are not provided.